Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2014–2015

27 859 Modernisering Gemeentelijke Basisadministratie persoonsgegevens (GBA)

Nr. 81 BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 10 september 2015

In mijn brief van 3 maart 2014 (Kamerstuk 26 643, nr. 307) heb ik u geïnformeerd over mijn voornemen om het mogelijk te maken de broncode van de Basisregistratie personen (BRP) in te zien. Tijdens het Algemeen Overleg van 27 november 2014 over de BRP (Kamerstuk 27 859, nr. 74) heb ik u toegezegd om de Kamer deelgenoot te maken van de ervaringen met de eerste inzageronde. Met deze brief geef ik invulling aan die toezegging en rapporteer ik over de ervaringen met die inzageronde, die in juni 2015 heeft plaatsgevonden.

Doel van de inzage in de broncode van de BRP

Operatie BRP draagt zorg voor de realisatie en de implementatie van de nieuwe technische voorzieningen voor het bijhouden en verstrekken van persoonsgegevens, de Basisregistratie Personen (BRP). Inzage in de broncode van de BRP is een goede manier om een «gratis kwaliteitscontrole» te organiseren waarbij externe partijen kwetsbaarheden in de software kunnen melden. Het is ook een goede manier om inzicht te bieden in de voortgang van de bouw van de software. Het gaat daarom bij de inzage om werkende delen van de BRP.

Aanpak van de inzage

Bij het bieden van de mogelijkheid de broncode van de BRP in te zien ga ik voorzichtig en stapsgewijs te werk. Ik heb u dat in maart 2014 geschreven en we hebben hierover in de Kamer ook enkele malen met elkaar van gedachten gewisseld. Ik heb u verteld dat ik zo open als mogelijk te werk ga, maar tegelijk in eerste instantie liever iets te voorzichtig ben dan dat ik te grote stappen zet. In de BRP zullen immers de persoonsgegevens van alle inwoners van Nederland zijn opgeslagen.

kst-27859-81
ISSN 0921 - 7371
's-Gravenhage 2015

Om de beveiliging van de BRP en de daarin opgeslagen persoonsgegevens te waarborgen gebeurt het vrijgeven voor inzage onder een aantal voorwaarden die ik in mijn brief van 3 maart 2014 heb beschreven. Een van die voorwaarden is dat de partijen die inzage krijgen met mijn ministerie een overeenkomst voor «responsible disclosure» sluiten. Die overeenkomst regelt het op verantwoorde wijze openbaar maken van (eventuele) kwetsbaarheden zodat operatie BRP deze op gecontroleerde wijze kan oplossen.

Ik schreef u eerder (Kamerstuk 27 859, nr. 77) dat ik me door uw Kamer heb laten overtuigen om geen «security by obscurity» toe te passen en dat ik, anders dan ik eerder van plan was, de delen van de code die de beveiliging betreffen ook beschikbaar stel voor inzage, uiteraard zonder de sleutels en andere technische informatie die nodig zijn om daadwerkelijk toegang tot de BRP te krijgen.

Tenslotte heb ik aangegeven dat iedereen zich kan aanmelden om inzage in de broncode te krijgen. De broncode wordt beschikbaar gesteld in een gesloten ruimte op een locatie van het Ministerie van BZK. De inzage heeft betrekking op een niet-gecompileerde versie van de broncode.

Verloop van de eerste inzageronde

Vanaf maart 2015 heeft Operatie BRP op de programmawebsite en in de nieuwsbrieven melding gemaakt van de mogelijkheid tot inzage en konden belangstellenden zich aanmelden. In mijn brief aan uw Kamer van april 2015 (Kamerstuk 27 859, nr. 78) heb ik melding gemaakt van de inzagemogelijkheid en dit is ook ter sprake gekomen in het Algemeen Overleg dat ik op 20 mei 2015 met uw Kamer voerde.

Vier partijen hebben zich aangemeld. Met twee van deze partijen is er na ontvangst van hun aanmelding, ondanks herhaalde pogingen van het programma, geen contact meer geweest. De andere twee partijen hebben in juni 2015 daadwerkelijk inzage in de broncode van de BRP gekregen.

Deze twee partijen hebben geen kwetsbaarheden in de broncode aangetroffen. Een van beide partijen heeft wel vier bevindingen gemeld: deze betreffen de wijze van coderen en het gebruik van versies van externe bibliotheken. Geen van de bevindingen had betrekking op kwetsbaarheden. Het programma heeft deze partij geïnformeerd over de wijze waarop deze bevindingen zijn of worden afgehandeld. De andere partij heeft aangegeven geen kwetsbaarheden te hebben aangetroffen en heeft geen bevindingen gemeld.

Een van beide partijen heeft via het beschikbaar gestelde evaluatieformulier enkele suggesties gedaan voor een volgende inzageronde, waaronder de suggestie om meer documentatie ter beschikking te stellen. De andere partij heeft geen gebruik gemaakt van de aangeboden mogelijkheid om bij te dragen aan de evaluatie van de inzage van de code.

Evaluatie van de inzage in de broncode

Operatie BRP heeft na afloop van de eerste inzageronde een verslag opgesteld van het verloop van de inzageronde. De belangrijkste punten daaruit heb ik hierboven beschreven. Ik heb daarna KPMG gevraagd om ook een evaluatie uit te voeren van deze inzageronde. De rapportage van

KPMG stuur ik u als bijlage bij deze brief toe[1]. De belangrijkste bevindingen en adviezen vindt u hieronder.

Bevindingen KPMG

- Operatie BRP heeft in het kader van de interne evaluatie een duidelijk feitenrelaas opgesteld van de voorbereiding, de uitvoering en afronding van de inzage. De interne evaluatie is niet opgesteld als een evaluatie van de doelstelling van de inzage.
- De overeenkomst voor responsible disclosure (RD) heeft goed gefunctioneerd conform de «Leidraad Responsible Disclosure» van het Nationaal Cyber Security Centrum (NCSC). Alle partijen hebben zich gehouden aan de afspraken in de overeenkomst inzake RD. KPMG plaatst wel enkele kanttekeningen in zijn rapport.
- Ten aanzien van de doelstelling «gratis kwaliteitscontrole» is de inzageronde nuttig gebleken. De gedane bevindingen zijn, hoewel in aantal beperkt, relevant. De bevindingen waren al bekend uit eerdere software kwaliteitschecks. De bevindingen blijven nuttig omdat hiermee aanvullende zekerheid is verkregen dat er geen aanvullende kwetsbaarheden in de code geconstateerd zijn.
- De inzage heeft ook ten aanzien van de doelstelling »transparant zijn over de voortgang» waarde: werkende stukken software kunnen worden ingezien en worden beschouwd in relatie tot de stapsgewijze ontwikkeling zoals vastgelegd in het Opleverplan van de BRP (BOP).
- KPMG wijst er op dat de inzage in de broncode slechts één van de elementen is waarmee inzicht in de voortgang van het programma kan worden verkregen. De Tweede Kamer wordt immers ook op andere manieren op de hoogte van de voortgang van operatie BRP gebracht, zoals bijvoorbeeld met de voortgangsbrieven. KPMG merkt op dat het Ministerie van BZK rond Operatie BRP een relatief grote mate van publieke transparantie nastreeft: «Zo is oBRP van de tien financieel meest omvangrijke ICT-projecten op het Rijks ICT Dashboard, het enige project dat over een eigen website met publieksinformatie beschikt (...). Op deze website staan niet alleen stukken die logischerwijs openbaar zijn (...) maar ook gedetailleerde, interne documenten (...). Ook is oBRP het eerste programma in Nederland dat kwaliteitstoetsen via een website openbaar maakt en broncode ter inzage heeft aangeboden.»

Advies KPMG

KPMG merkt naar aanleiding van de hiervoor vermelde bevindingen op dat het voor de hand ligt om ook in volgende fasen van de bouw inzageronden te organiseren. Voor die volgende inzageronden doet KPMG de aanbevelingen om:
- inzage te verlenen na afronding van iedere stap uit het BRP-Opleverplan waarin een werkende versie van de software wordt opgeleverd;
- meer belangstelling voor de inzage te genereren door de juiste kanalen aan te boren;
- meer feedback te genereren door specifiekere vragen te stellen en een gesprek te voeren met iedere partij die inzage heeft gehad;
- deze beide aanpassingen in het plan van aanpak te verwerken en daarin ook duidelijker aan te geven dat er bij de inzage documentatie ter beschikking wordt gesteld die inzicht geeft in de opzet en structuur van de broncode.

[1] Raadpleegbaar via www.tweedekamer.nl

KPMG adviseert voorts om na afronding van de ontwikkeling van de BRP de wijze van openbaar maken van de code voor inzage te heroverwegen. Daarbij merkt KPMG het volgende op: «Bij systemen die, zoals de BRP, een hoge mate van vertrouwelijkheid en integriteit vereisen, kunnen er mogelijk redenen zijn om niet, of niet meteen, de volledige broncode te openbaren. (...) Een alternatieve methode voor omgang met deze trade-off tussen openbaarheid en vertrouwelijkheid is een gesloten gemeenschap. Zo heeft Denemarken een systeem waarbij open source software in een centraal register (...) wordt geplaatst wat toegankelijk is voor alle overheidsorganisaties voor hergebruik en evaluatie, maar niet daarbuiten.».

Tot slot beveelt KPMG aan om na afronding van het programma de afweging te maken of de broncode, en zo ja welk deel daarvan, als open source software beschikbaar wordt gesteld. Daarbij wijst KPMG op enkele aandachtspunten en merkt op:
- dat de software van operatie BRP door het bieden van inzage of openbaar maken niet noodzakelijkerwijs zelf open source wordt en dat ook het gebruik maken van open source middelen door operatie BRP de ontwikkelde software niet open source maakt;
- dat gezien de aard van de functionaliteit van de BRP niet te verwachten is dat er veel behoefte voor hergebruik van de software van de BRP is.

Vervolg van de inzage in de broncode BRP

Op basis van de eerste ervaringen met de inzage en de bevindingen en het advies van KPMG heb ik besloten dat ik met het vrijgeven van de broncode voortga op de ingeslagen weg maar wel met enkele aanpassingen.

Zoals eerder gemeld zal ik periodiek, bij oplevering van werkende versies van de software, de mogelijkheid tot inzage in de broncode bieden. Het blijft dus niet bij deze eerste ronde van inzage, er zullen nog enkele inzagerondes volgen.

De eerstvolgende inzage kan plaatsvinden op de volgende werkende versie van de BRP, dat is de software voor de mutatieleveringen die wordt gerealiseerd in ontwikkelstap 3.1[2]. Deze is per 1 oktober 2015 beschikbaar voor het acceptatietraject. Ik wil die volgende inzageronde uiterlijk begin 2016 laten plaatsvinden.

Daarbij zal ik op hoofdlijnen dezelfde procedure en voorwaarden hanteren die nu gelden, waaronder het tekenen van een overeenkomst voor «responsible disclosure». Indachtig de suggesties van KPMG zal ik Operatie BRP opdragen om voor het bekend stellen van de inzage ook andere kanalen te gebruiken teneinde meer belangstelling te genereren. Ook de andere in deze brief genoemde suggesties voor aanpassing van de procedure neem ik over.

Voorafgaand aan het in productie gaan van de BRP zal ik opnieuw evalueren en mijn beleid rondom de openbaarheid van de broncode van de BRP vaststellen op basis van de ervaringen die ik in de inzagerondes heb opgedaan.

---

[2] Op www.operatiebrp.nl staat het BRP Opleveringsplan (BOP), waarin alle ontwikkelstappen met nummering terug te vinden zijn.

Ik zal uw Kamer in de reguliere voortgangsrapportages van Operatie BRP steeds informeren over de stand van zaken met betrekking tot de inzagerondes. De eerstvolgende voortgangsrapportage stuur ik u over ongeveer een maand.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk